## CLAIMS

**1.** A system comprising:

- an output device for outputting data onto a removable storage medium;
- a first computing entity arranged to encrypt a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set onto a said removable storage medium, the first computing entity being further arranged to output the encrypted first data set for the output device; and
- a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the output device a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data;

the output device being arranged to use the decryption key in decrypting the encrypted first data set.

**2.** A system according to claim 1, wherein the second computing entity is arranged to generate the decryption key only when said policy has been met.

**3.** A system according to claim 1, wherein the second computing entity is arranged to issue to the first computing entity at least one of:

- the second data set;
- the encryption key string;
- a derivative of the encryption key string usable by the first computing entity, in place of the encryption key string, in the encryption of said first data set.

**4.** A system according to claim 1, wherein the second computing entity is arranged to receive the encryption key string directly or indirectly from the first computing entity.

**5.** A system according to claim 1, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising for the or each said further trusted party the public data of that trusted party and a respective further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; the or each further second computing entity being arranged, when satisfied that the policy defined by the encryption key string related to the associated trusted party has been met, to provide a further decryption key to the output device, the second computing entity concerned being arranged to generate this further decryption key in dependence on the private data and encryption key string corresponding to the associated trusted party; and decryption of the encrypted first data set by the output device requiring use of the decryption keys provided by all of the trusted parties.

**6.** A system according to claim 5, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the output device is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the output device.

**7.** A system according to claim 5, wherein the first computing entity is arranged to process the first data set, prior to encryption, to form a plurality of

data strings, the first computing entity being further arranged to encrypt each data string based on the encryption parameters associated with a respective one of the trusted parties, and the output device being arranged to decrypt each string using the decryption key provided by the related trusted party and then to process the strings to recover the first data set.

**8.** A system according to claim 1, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising the public data of the or each further trusted party; each second computing entity being arranged, when satisfied that the policy defined by the encryption key string has been met so far as the associated trusted party is concerned, to provide a respective decryption key to the output device, the second computing entity concerned being arranged to generate this decryption key in dependence on the encryption key string and the private data of the associated trusted party; and decryption of the encrypted first data set by the output device requiring use of the decryption keys provided by all of the trusted parties.

**9.** A system according to claim 8, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each second computing entity being arranged to be satisfied that said policy has been met when the set of at least one condition for the trusted party associated with the second computing entity concerned has been met.

**10.** A system according to claim 8, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the output device is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the

document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the output device.

**11.** A system according to claim 1, wherein the first data set is encrypted using a bilinear pairing technique.

**12.** A system according to claim 1, wherein the first data set is encrypted using a quadratic residue technique.

**13.** A system according to claim 1, wherein the output device and the second computing entity are incorporated into the same item of equipment.

**14.** A system according to claim 1, further comprising a portable device comprising the second computing entity and a first communications interface, the output device comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the output device; the communications interfaces being such that the portable device must be present at the output device for the communication between the second computing entity to take place.

**15.** A data output method comprising the steps of:

(a) encrypting a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string comprising a second data set that defines a policy for allowing the output of the first data set to a removable storage medium,

(b) providing the encrypted first data set to an output device adapted to output data to a removable storage medium;

(c) at the trusted party checking that said policy has been satisfied and thereafter providing the output device with a decryption key for use in

decrypting the encrypted first data set, this decryption key being generated in dependence on the encryption key string and private data related to said public data; and

(d) at the output device using the decryption key in decrypting the encrypted first data set and outputting the first data set to a removable recording medium.

**16.** A method according to claim 15, wherein in step (c) the decryption key is generated only after said policy has been satisfied.

**17.** A method according to claim 15, further comprising an initial step of generating the second data set at the trusted party and providing to a party that is to carry out step (a) at least one of:

- the second data set;
- the encryption key string;
- a derivative of the encryption key string usable in step (a), in place of the encryption key string, in the encryption of said first data set.

**18.** A method according to claim 15, wherein the trusted party receives the encryption key string directly or indirectly from a party that carries out step (a).

**19.** A method according to claim 15, wherein:

- in step (a) said encryption parameters further comprise public data of at least one further trusted party and a respective related further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set;
- in step (c) the or each further trusted party, when satisfied that the policy defined by the related encryption key string has been met, provides a further decryption key to the output device, the further trusted party concerned generating this further decryption key in dependence on private data and said related encryption key string; and

- in step (d) decryption of the encrypted first data set by the output device requires use of the decryption keys provided by all of the trusted parties.

**20.** A method according to claim 19, wherein:

- the first data set concerns a document to be published;
- step (a) is carried out by a document publisher who also serves as one of the trusted parties;
- the output device is associated with a document seller;
- in step (c) the trusted party associated with the document publisher checks satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and
- in step (c) another of said trusted parties checks satisfaction of at least one condition concerning the output device.

**21.** A method according to claim 19, wherein:

- in step (a) the first data set is processed, prior to encryption, to form a plurality of data strings, each string being thereafter encrypted based on the encryption parameters associated with a respective one of the trusted parties, and
- in step (d) the output device decrypts each string using the decryption key provided by the related trusted party and then processes the strings to recover the first data set.

**22.** A method according to claim 15, wherein:

- in step (a) said encryption parameters further comprise public data of at least one further trusted party;
- in step (c) each trusted party, when satisfied that the policy defined by the encryption key string has been met so far as it is concerned, provides a respective decryption key to the output device, the further trusted party concerned generating this decryption key in dependence on private data and the encryption key string; and

- in step (d) decryption of the encrypted first data set by the output device requires use of the decryption keys provided by all of the trusted parties.

**23.** A method according to claim 22, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each trusted party being arranged to be satisfied that said policy has been met when the set of at least one condition associated with the trusted party has been met.

**24.** A method according to claim 22, wherein:

- the first data set concerns a document to be published;
- step (a) is carried out by a document publisher who also serves as one of the trusted parties;
- the output device is associated with a document seller;
- in step (c) the trusted party associated with the document publisher checks satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and
- in step (c) another of said trusted parties checks satisfaction of at least one condition concerning the output device.

**25.** A method according to claim 15, wherein in step (a) the first data set is encrypted using a bilinear pairing technique.

**26.** A method according to claim 15, wherein in step (a) the first data set is encrypted using a quadratic residue technique.

**27.** A method according to claim 15 wherein the trusted authority is implemented in a portable device arranged to communicate with the output device only when the portable device is present at the output device.

**28.** A printing system comprising:

- a printer;
- a first computing entity arranged to encrypt a first data set based on encryption parameters comprising public data of a trusted party and an encryption key string comprising a second data set that defines a policy for allowing the printing of the first data set, the first computing entity being further arranged to output the encrypted first data set for the printer; and
- a second computing entity associated with the trusted party and arranged when satisfied that said policy has been met, to output for the printer a decryption key for use in decrypting the encrypted first data set, the second computing entity being arranged to generate this decryption key in dependence on the encryption key string and private data related to said public data;

the printer being arranged to use the decryption key in decrypting the encrypted first data set.

**29.** A system according to claim 28, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising for the or each said further trusted party the public data of that trusted party and a respective further encryption key string that comprises further second data defining a further policy for allowing printing of the first data set; the or each further second computing entity being arranged, when satisfied that the policy defined by the encryption key string related to the associated trusted party has been met, to provide a further decryption key to the printer, the second computing entity concerned being arranged to generate this further decryption key in dependence on the private data and encryption key string corresponding to the associated trusted party; and decryption of the encrypted first data set by the printer requiring use of the decryption keys provided by all of the trusted parties.

**30.** A system according to claim 29, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the printer is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the printer.

**31.** A system according to claim 29, wherein the first computing entity is arranged to process the first data set, prior to encryption, to form a plurality of data strings, the first computing entity being further arranged to encrypt each data string based on the encryption parameters associated with a respective one of the trusted parties, and the printer being arranged to decrypt each string using the decryption key provided by the related trusted party and then to process the strings to recover the first data set.

**32.** A system according to claim 28, further comprising at least one further second computing entity associated with a respective further trusted party that has related public and private data, said encryption parameters further comprising the public data of the or each further trusted party; each second computing entity being arranged, when satisfied that the policy defined by the encryption key string has been met so far as the associated trusted party is concerned, to provide a respective decryption key to the printer, the second computing entity concerned being arranged to generate this decryption key in dependence on the encryption key string and the private data of the associated trusted party; and decryption of the encrypted first data set by the printer requiring use of the decryption keys provided by all of the trusted parties.

**33.** A system according to claim 32, wherein said policy comprises a respective set of at least one condition associated with the or each trusted party, each second computing entity being arranged to be satisfied that said policy has been met when the set of at least one condition for the trusted party associated with the second computing entity concerned has been met.

**34.** A system according to claim 32, wherein the first data set concerns a document to be published, the first computing entity and one of the second computing entities are both associated with a document publisher, and the printer is associated with a document seller; the second computing entity associated with the document publisher being arranged to check satisfaction at least of a policy condition requiring notification of details of the document and seller to the document publisher, and a further said second computing entity being arranged to check satisfaction of at least one policy condition concerning the printer.

**35.** A system according to claim 28, wherein the first data set is encrypted using a bilinear pairing technique.

**36.** A system according to claim 28, wherein the first data set is encrypted using a quadratic residue technique.

**37.** A system according to claim 28, wherein the printer and the second computing entity are incorporated into the same item of equipment.

**38.** A system according to claim 28, further comprising a portable device comprising the second computing entity and a first communications interface, the printer comprising a second communications interface arranged to cooperate with the first communications interface to enable communication between the second computing entity and the printer; the communications

interfaces being such that the portable device must be present at the printer for the communication between the second computing entity to take place.

**39.** Printing apparatus including:

- means for receiving both an encryption key string comprising policy data defining a policy for allowing the printing of payload data, and said payload encrypted based on encryption parameters comprising public data of a trusted party and said encryption key string;
- means for providing the encryption key string to the trusted authority and for receiving back a decryption key; and
- means for using the received decryption key in decrypting the encrypted payload data for printing.

**40.** An item of equipment comprising printing apparatus according to claim 39, and a computing entity arranged to serve as said trusted party.